The War of Ideas and the Role of Information Operations in Counterinsurgency

A Monograph

by

MAJ Collin T. Hunton

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 06-07

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
27-04-2007	MONOGRAPH	Sep 2006- Mar 2007

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The War of Ideas and the Role of Information Operations in Counterinsurgency	
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
MAJ Collin T. Hunton	
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
School of Advanced Military Studies 250 Gibbon Avenue Ft. Leavenworth, KS 66027	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
Command and General Staff College 1 Reynolds Avenue Ft. Leavenworth, KS 66027	CGSC, SAMS
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

See Attached Abstract.

15. SUBJECT TERMS

Information Operations, Counterinsurgency

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	(U)		COL Kevin Benson
(U)	(U)	(U)		52	19b. TELEPHONE NUMBER *(Include area code)* (913) 758-3300

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Collin Trent Hunton

Title of Monograph: The War of Ideas and the Role of Information Operations in Counterinsurgency
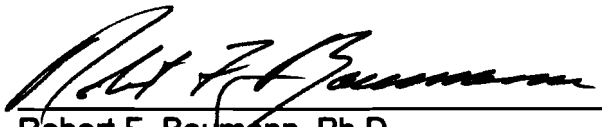
Approved by:

_____ Monograph Director
Rick M. Beckinger, COL, AV

_____ Director,
Kevin C.M. Benson, COL, AR   School of Advanced
                                   Military Studies

_____ Director,
Robert F. Baumann, Ph.D.   Graduate Degree
                                   Programs

Abstract

The War of Ideas and the Role of Information Operations in Counterinsurgency, by MAJ Collin T. Hunton, United States Army, 59 pages.

Since the attacks of September 11, 2001, the United States' armed forces and its coalition of allies have become deeply entrenched in the counterinsurgencies of Iraq and Afghanistan. These struggles are not just counterinsurgencies, but they also represent the front lines of the nation's "War of Ideas" between Western ideology and Islamic extremism, where influence and management of perceptions is paramount. Because of the inherently political nature of counterinsurgency (COIN) operations coupled with the dynamics of conflict within the information age, the role of information operations (IO) has assumed a new level of importance.

As the US and its coalition partners continue their COIN efforts, it is clear that the increased role of IO relative to kinetic operations has been greatly misunderstood. This circumstance is due in large part to a lack of common understanding of IO concepts and definitions within the military community and a deficiency of coherent doctrinal guidance on how to properly integrate IO into COIN operations. In consideration of these doctrinal shortfalls, commanders who have been uncomfortable with the concept of IO have commonly subordinated its importance to the more tangible kinetic elements of COIN operations.

This monograph analyzes the historical development of US IO doctrine and provides a discussion of the way ahead for common understanding among the services. Investigation into Clausewitz's theory of political conflict helps to reinforce how the role of IO relates to kinetic operations based on the assessed nature of the conflict. Finally, an assessment of the new COIN manual FM 3-24, and analysis of the many considerations for proper understanding of the information environment provide scope to the challenges ahead for US forces in the COIN conflict.

The monograph identifies that while new Joint IO and Army COIN doctrines have provided a solid foundation for a change in understanding of the necessities for this contemporary conflict, there are still unresolved issues which may inhibit the commander's proper integration of IO. The monograph makes the following recommendations to improve the overall understanding and capability of IO within the current conflict. First, US Army IO doctrine must nest within the framework of the new Joint doctrine in order to gain and maintain momentum in this increasingly joint and interagency effort. Second, US Army IO and COIN doctrine should provide better methodology to the force for the application of all IO elements. Third, the US Army must improve the general education of IO across all branches and at every echelon of the service so the IO expertise does not rest solely within the IO career field. Fourth, the means for assessment and analysis between IO and military intelligence (MI) should work towards more complete integration to improve the comprehensiveness and timeliness of understanding. Finally, commanders must establish a proactive posture for their IO campaigns if they are to maintain the legitimacy of their overall COIN effort. The analysis, assessments and recommendations in this monograph provide a bridge of understanding between IO and COIN operations and highlight the importance of the proper integration of IO within the current conflict.

TABLE OF CONTENTS

Table of Figures

CHAPTER ONE
INTRODUCTION

Since the horrific attacks of September 11, 2001, the United States and its coalition of allies have been embattled in a clash which is not only re-defining the future of conflict, but is also helping to re-shape the government's and armed forces' organization and methods of operation.[1] The reasons for this dynamic shift are numerous, but the most significant reason rests with the emergence of state and non-state terrorist actors who have effectively used unconventional means to undermine the US' conventional military strength.

Prior to the fateful day in September, 2001, much had been written and discussed about the advent of the "information age" of warfare. The rhetoric had even generated some initial steps to transform US forces from the industrial age infrastructure of the Cold War to the more agile and efficient force designed for the information age paradigm. Such steps were manifested in the Force XXI, and Army After Next projects. Yet until the US found itself in the current asymmetric war there was no true catalyst to shake the collective thinking from the remains of the industrial age mindset. Subsequently, US organizations, both the armed forces and the civilian government, lagged behind in their transformations, and the Information Operations doctrine capable of supporting their transformations was slow to develop.

The information paradigm was not the only realm neglected during the twilight of the Cold War mentality. In a similar fashion, US policies and doctrine on counterinsurgency warfare were also ignored. Despite the US' significant history and experience in "small war" counter-insurgency campaigns, from Mexico, to the Philippines, Nicaragua, and Vietnam, our institutions seemed to have forgotten the many lessons learned at the expense of our nation's blood and treasure. In fact, since the conclusion of the Vietnam conflict, our armed forces took active

measures to sweep counterinsurgency warfare from our collective memories. Training and

Doctrine Command (TRADOC) resolutely omitted any mention of counterinsurgency from the

Army's 1976 benchmark war fighting *Field Manual (FM) 100-5 Operations*. Such actions gave

momentum to the movement that eventually became the "Weinberger doctrine" of 1983 which

was founded with the principle that the nation would never be committed to a counterinsurgency

again.[2]

The United States' armed forces are now deeply entrenched in the counterinsurgencies of

Iraq and Afghanistan. These struggles are not just counterinsurgencies, but they also represent

the front lines of the nation's "War of Ideas" between Western ideology and Islamic extremism,

where influence and management of perceptions is paramount.[3] This research monograph will

explore the role of information operations (IO) within contemporary operations and will identify

several reasons why commanders and staffs have been challenged to integrate IO into the ongoing

counterinsurgency (COIN) operations.

As the US and its coalition partners continue in their COIN efforts, it is clear that the role

of IO relative to kinetic operations has been greatly misunderstood. This circumstance is due in

large part to a lack of common understanding of IO concepts within the military community and a

lack of coherent doctrinal guidance on how to properly integrate IO into COIN operations. In

consideration of these doctrinal shortfalls, commanders who have been uncomfortable with the

concept of IO have routinely subordinated its importance to more tangible kinetic elements of

COIN operations. Because COIN operations are more political by nature, and the availability of

information in this era has increased exponentially, US efforts to inform and influence both the

---

[1]Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's Inc. 2004) 1.

[2]John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago, IL: University of Chicago Press, 2005), 206-7.

[3]William Roseneau, *Waging the War of Ideas*, Rand Corporation Reprint Series, Chapter 72 of the McGraw-Hill Homeland Security Handbook (Washington DC: McGraw-Hill, 2006), 1131-1148.

policy makers and the affected populations can no longer be considered as mere augmentation to the more tangible kinetic efforts of traditional military operations. Although the publication of the new COIN manual has provided the force with a fresh perspective and significant thoughts for the integration of IO in COIN operations, several considerations remain unresolved. This monograph will attempt to highlight some of the remaining issues and provide recommended solutions for the way ahead.

The departure point for discussion of the topic will be an examination of IO theory and doctrine. A review of joint and service IO doctrine and their disparate development will provide scope to the misunderstanding of IO between the services. This will be followed by a review of the Department of Defense's (DoD) 2003 *IO Roadmap*, which provided coherent policy and direction to settle the differences between the services and further established a common direction for the future of IO as a DoD core competency.

Delving into theory, the paper will provide an evaluation of the established principles of IO within COIN operations against the assertions of COL William Darley in his think piece *Clausewitz's Theory of War and Information Operations*. The premise of this comparison is that the role of IO relative to kinetic operations has been greatly misunderstood and has not adapted to the complexities of our current operations. Given the influence of policy at home and abroad within the asymmetric nature of COIN operations, a review of Clausewitz's theory of political conflict will help us understand the role of information operations as a more political activity with a significantly greater responsibility in COIN operations. This theoretical idea will provide the framework for the ideas offered throughout this monograph. Following an exploration of this theory, an evaluation of the IO principles included within the new COIN manual *FM 3-24 Counterinsurgency Operations* will establish a baseline for the remainder of the discussion.

The review of doctrine and theory will be followed by a review of the current information environment as it relates to the physical environment as well as a review of several timeless

3

considerations for employment of IO in COIN. This assessment will provide a contextual foundation for the challenges facing our forces in the current COIN environments of Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF).

The recommendations of the monograph will be based on the results of the research and within the context of the presented framework. They will focus on those conditions which continue to inhibit the proper integration of IO into the COIN operational planning and execution. The summary will provide key findings from the research question and should offer a useful framework for our operational and tactical commanders as they prepare for their deployments to either theater of our current conflict.

CHAPTER TWO
IO DOCTRINE

IO is not conceptually new. Sun Tzu highlighted the importance of information and mentioned the use of counterintelligence agents, deception and psychological operations in great detail throughout his work.[4] Napoleon himself was a master of deception and other elements of IO. Throughout his campaigns Napoleon regularly implemented secondary offensives and various psychological operations practices in conjunction with efforts to control and "tune" the press to create the perceptions he wanted his adversaries to gain.[5] In fact, there have been examples throughout military history of the effective use of the various elements of IO. Yet despite a long standing presence and importance of these elements within the armed forces, the umbrella concept of IO does not have a long doctrinal history. What history it does have has been filled with a broad range of commentary and perspective. This chapter will attempt to give the reader an understanding of the concept of IO, present a short synopsis of how the military community arrived at the current doctrine for the concept, and set the stage to demonstrate how the disparity among the services understanding of IO may have hindered our ability to create synergy in our overall operations.

To begin the discussion we might ask "what is IO?", and to that question, there has not been a truly straight forward answer. *Joint Publication 3-13 Information Operations*, published 13 February 2006, defined IO as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision

---

[4]Samuel B. Griffith, *The Art of War: Sun Tzu* (New York: Oxford University Press, 1963), Chapter 1 discussion on estimates, 63-66; Chapter 13 discussion of the use of agents for the collection and distribution of information, 144-149.

making while protecting our own."[6] This relatively recent definition encompasses all current elements of IO and provides reference to its related activities. Yet while it provides the military professional with a concise definition, if someone were to ask the question "what is IO?" to one-hundred different service members across all services, they would still likely get ninety-nine different answers. The reasons for the disparity are numerous, but perhaps the most significant reason for the different understanding is the abstract and duplicitous nature of the subject.

IO is about influence and management of perceptions. It is also about decision making in the knowledge war and is both offensive and defensive. As an offensive weapon IO is a means to multiply potential power and strength, yet at the same time, if not defended properly, it is one of our most critical vulnerabilities.[7] To further complicate things, IO exists and operates simultaneously in three different dimensions; the physical, the informational and the cognitive, and it does so across all three levels of war, often blurring the lines between strategic, operational and tactical. So not only does IO have a self-conflicting nature, but it is at once involved everywhere, across the spectrum of conflict, in every aspect of military operations. It is because of this complicated existence that IO has remained mysterious and difficult for the joint community to establish a definition agile enough to satisfy all the services and their functional areas at all levels of warfare.

The first step in understanding IO is to examine the current joint doctrine to establish the baseline understanding of how IO is defined. Despite the broad arrangement of commentary on the subject, the definitions and principles offered in the latest Joint Publication (JP) 3-13, *Information Operations*, published 13 February 2006 will be used to establish the baseline understanding for this paper. This overarching doctrinal manual updates the definitions and

---

[5]David G. Chandler, *The Campaigns of Napoleon* (New York: MacMillan Publishing), 146.
[6]U.S. Deparment of Defense Joint Publication 3-13, *Information Operations*, 13 February 2006, I-1.

principles from its preceding version published in October, 1998. As a starting point, the new JP

3-13 establishes IO as a means to achieve Information Superiority, with its key goal of enabling

superior decision making and thereby providing the operational commander a marked

competitive advantage.[8] As stated earlier JP 3-13 defines IO as "the integrated employment of

electronic warfare (EW), computer network operations (CNO), psychological operations

(PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with

specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial

human and automated decision making while protecting our own."[9] This definition identifies the

five core elements of IO, but more importantly it also identifies the need for the various

supporting and related activities to be incorporated synergistically in order to accomplish its

purpose of diminishing adversarial information, while simultaneously enabling and protecting our

own information. Because of the close relation between the core elements and the supporting and

related activities, and the risk for information fratricide, the integration of all the activities is

critical to successful incorporation of the IO concept throughout the information environment and

all levels of warfare.

With the definition established, JP 3-13 proceeds to describe the information

environment. The doctrinal baseline for the concept is defined as "the aggregate of individuals,

organizations, and systems that collect, process, disseminate, or act on information, where the

actors include leaders, decision makers, individuals, and organizations."[10] While the information

environment is distinct, it resides in all aspects of the decision making cycle and is made up of

three separate dimensions, the physical, the informational and the cognitive. The physical

---

[7]Wayne Michael Hall, *Stray Voltage: War in the Information Age* (Annapolis, MD: Naval Institute Press, 2003), 100.
[8]Joint Publication 3-13, I-1.
[9]Ibid.
[10]Ibid.

dimension is comprised of the command and control systems and supporting infrastructure that enable individuals and organizations to conduct operations within their physical domains. The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected. Finally, the cognitive dimension encompasses the mind of the decision maker and the target audience (TA).

Of the three dimensions of the information environment, the cognitive is the dimension in which people think, perceive, visualize, and decide.[11] Because of its abstract nature, the cognitive dimension is at once the most important and also the most difficult of the three dimensions to truly dominate for any significant length of time. In today's informational environment perceptions and attitudes are shaped by a continuous stream of new information all vying to gain influence over the cognitive terrain. A contextual exploration into the current information environment later in this paper will highlight some of the major challenges associated with the cognitive dimension in our current operations. With some perspective on the current joint doctrinal definitions we will next try to gain greater perspective of the current issues surrounding IO by examining how the concept first came into being.

Disparate Beginnings of IO Doctrine

Following Operation Desert Storm in 1991 most of the core elements of what is now known as IO were bound by the moniker of Command and Control Warfare (C2W). The core elements of C2W included a collection of some of the contemporary elements such as electronic warfare (EW), military deception (MILDEC), operational security (OPSEC), psychological operations (PSYOP), along with a variant of the current supporting activity of physical attack, which was at the time coined C2W physical destruction.[12] The C2W concept was introduced as

---

[11]Ibid., I-2.
[12]U.S. Department of Defense Directive 3222.4, *Electronic Warfare (EW) and Command and Control (C2W) Countermeasures,* 31 July 1992.

an effort to capitalize on the lessons learned from Operation Desert Storm which was for some the first war waged in this new "Information Age."[13] Except for this previous grouping of IO core elements into C2W, the concept of IO was still not fully defined in any military circles until the publication of the Army's Training and Doctrine Command (TRADOC) Publication 525-69, dated 1 August, 1995. While this document was not the first to mention IO as a concept, it was the first to discuss the concept with any depth. TRADOC Pub 525-69 set the stage for the Army to embrace the "Information Age" technologies which first saw extensive use in Operation Desert Storm. This publication provided commanders below the strategic level an initial methodology to integrate both the offensive and defensive aspects of the IO concept as an enabling means for future military operations.[14] Although this initial publication gained wide acceptance and many agreed with the necessity to explore and incorporate IO into the battlefield framework, there was still not enough intellectual momentum across the services to make the necessary institutional changes to properly incorporate the concept. Yet by this time, the joint community and most of the services had already begun shaping their own versions of the emerging doctrine.

The concept of IO next appeared in the 1996 publication of *Joint Vision 2010 (JV 2010)*. JV 2010 used proscriptive language to focus the services on leveraging innovative technologies to achieve new levels of effectiveness and full-spectrum dominance. Although the document spent ample time discussing the importance of information and information technologies, its focus was almost exclusively on the concept of "Information Superiority" (IS). JV 2010 defined IS as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[15] IO, on the other hand, was only

---

[13]Armistead, 16.
[14]U.S. Army TRADOC Pamphlet 525-69, 1 August 1995.
[15]U.S. Joint Chiefs of Staff, *Joint Vision 2010*, (Washington, DC: GPO, July 1996).

briefly mentioned in JV 2010 as the means to achieve the "end" of IS, and the concept still lacked

any concrete definition or conceptual framework.

While Information Operations was not specifically defined within JV 2010, in December

1996, the Department of Defense released the Department of Defense Directive S-3600.1,

Information Operations, and established IO as an instrument of military operations to gain and

maintain information dominance.[16] Concurrently, the US Army attempted to quickly establish

their own framework for the concept and became the first service to publish its own doctrinal

manual, Field Manual 100-6, *Information Operations* in August 1996. For the Army, this manual

took the existing concepts of C2W, and for the first time consolidated the related activities of

Civil Affairs, and Public Affairs under one heading, necessitating their coordination in order to

achieve a common direction.[17] The manual also became the first to fully describe the intricacies

of the information environment and its importance to the Intelligence Preparation of the

Battlefield (IPB) process for planning and executing military operations. Where the Army's first

IO manual failed was in adequately prescribing the methodology necessary to properly integrate

IO into plans and operations. There were seemingly no procedures, dedicated staff actions or

assigned responsibilities to any Army staff sections. Although the Army made great progress in

giving shape to the concept of IO, its role within planning and execution was minimized by

commanders and staffs who were not completely familiar or comfortable with the concept's

integration.[18]

---

[16]DOD Directive S-3600.1. This policy was declassified from TS in Dec. 1996 in order to broaden the collective understanding of the IO concept within the military and civilian communities. The document introduced CNA as a function of IO. The directive is still classified For Official Use Only (FOUO).

[17]U.S. Army Field Manual 100-6, *Information Operations*, 27 August 1996.

[18]Charles N. Eassa, "US Armed Forces Information Operations: Is the Doctrine Adequate?" (Monograph, School of Advanced Military Studies, USACGSC, Fort Leavenworth, KS, First Term, AY 99-00), 20.

Two years later, in October 1998, the Office of the Joint Chiefs of Staff published Joint Publication 3-13, *Information Operations*. This manual offered all the armed services an overarching foundation from which they could individually depart to construct their own doctrine. Unfortunately by this time, each of the individual services had already begun developing their own roles for IO in manners best suited for their own capabilities. While each service's effort was not altogether inconsistent with the Joint Publication's general direction, they didn't necessarily develop in a synchronized manner. A review of each of the service's conceptual development will provide scope to the disparity in the joint community.

The Air Force established its IO doctrine through the publication of *Air Force Doctrinal Document (AFDD) 2-5* in August 1998. While this was the first formal Air Force publication dedicated specifically to IO, the Air Force was already well established with Information Warfare (IW) capabilities even having established the Air Force Information Warfare Center in 1993.[19] Published two months before JP 3-13, the AFDD 2-5 discussed the importance of information operations across the spectrum of conflict. Despite this commitment to the full-spectrum, the Air Force publication seemed to focus predominately within the realm of existing conflict. This tendency can easily be attributed to the Air Force's roles within the different phases of the battlefield framework. For example, what is considered pre-hostility action or Flexible Deterrent Options (FDO) within the overarching strategic framework generally translates to hostile action by those Air Force elements conducting them. Still, the Air Force was attempting to provide doctrine with similar language to the joint publication. A summary of AFDD 2-5 will provide some of the Air Force's individual developments within IO doctrine.

Beginning at the strategic level, AFDD 2-5 mentioned the necessity of tying its efforts into the Defense Information Infrastructure (DII), the National Information Infrastructure (NII)

---

[19]Ibid., 14.

and the Global Information Infrastructure (GII). Consistent with the joint references, AFDD 2-5 described these three hierarchies individually as those information systems architectures which serve the informational needs within the local defense, and national and global information arenas.[20]

Despite this reference to nesting into the three levels of the strategic architecture, the preponderance of the document's dialogue focused narrowly on the concept of its "two pillars"; information-in-war (IIW), and information warfare (IW). In accordance with AFDD 2-5, IIW related to those aspects of information management impacting the commander's information requirements in support of making decisions. These elements included Intelligence, Surveillance and Reconnaissance (ISR), weather, precision and global positioning system capability (GPS).

Meanwhile IW, coinciding with the Joint Doctrine elements of IW, had both offensive and defensive categorizations. The offensive category included Psychological Operations (PSYOP), military deception, physical attack and informational attack. Conversely, the defensive category included information assurance, Operational Security (OPSEC), counterintelligence, counter PSYOP, electronic protection, and counter deception.[21] Although some defensive elements of IW operate outside of the spectrum of conflict, IW as a whole is generally associated with activities within combat operations.[22]

AFDD 2-5 mentions the need to incorporate IO throughout the full spectrum of operations; however, the Air Force's first attempt at conceptualizing IO was still almost entirely rooted in its IW capabilities.[23] With exception of the Air Force's support to PSYOP, its IO effort remained focused primarily in the electronic spectrum, and operated in the physical and informational dimensions of the information environment. While this focus is consistent with the

---

[20]U.S. Air Force *Doctrinal Document 2-5*, 5 August 1998, 5.
[21]Ibid., 3.
[22]Armistead, 19.
[23]Eassa, 14.

Air Force's traditional role of air and space dominance, its initial installment was not truly full-spectrum, as it failed to address the important aspects of pre and post-conflict information activities.

The Navy created very little prescriptive doctrine to guide its IO activities, but similar to its sister services, a thread of common language and understanding existed. For the Navy, IO was and until very recently continued to be considered synonymous to C2W and the Navy's development of IO has been consistent with its unique role within the force.[24] The Navy's development of the concept was significantly influenced by several factors. The first influence was the Navy's extremely technical orientation and vast amount of information required to conduct its primary mission of securing the sea lines of communication. Additionally, because the Navy's operations are centralized within the various operational task groups, there is a significant need for the critical operational information to be centrally controlled and managed. Thus, the Navy's focus in the information realm was predominately defensive in scope and focused on information protection.[25] Like the Air Force, the Navy's traditional focus on dominance of the sea and its inherently technical orientation has restricted its focus of IO within the physical and informational dimensions.

Like the other services the US Marine Corps had also publicly acknowledged the need for the development of information operations concepts for its own operations, and in May 1998 published a white paper, "A Concept for Information Operations." This article, like much of the Marine Corps doctrine, followed very closely to the established principles found within the Army's FM 100-6, designating offensive and defensive tenets and integrating the related activities of public affairs and civil-military operations.[26] Although it was a very brief article, it

---

[24]Ibid., 15.
[25]Ibid., 16.
[26]J. E. Rhodes, "A Concept for Information Operations," *Marine Corps Gazette*, August 1998, A-4-5.

was well written and provided the Marine Corps direction for making the required doctrinal, organizational, educational, training and equipping changes for successful integration of IO across the full spectrum of operations. Unfortunately, the Marine Corps has still failed to publish their own complete doctrinal manual, and has only released a final coordinating draft of Marine Corp Warfighting Publication (MCWP) 3-36, *Information Operations* in February 2001.[27]

Having reviewed all of the services initial efforts to define the concept of IO, it is evident that there was significant disparity between the services' conceptual IO framework. As noted earlier, the Navy and Air Force's role within the joint community is traditionally focused on the dominance of their own unique physical dimensions be it the sea, or air and space. Subsequently and not surprisingly, the developments of their IO capabilities mirrored their focus and were thus limited within their specific physical dimensions of expertise.

The Army and Marine Corps on the other hand not only needed to dominate their own terrain-based physical domains, but because of greater potential interaction with civilian populations, they also focused on the capability to operate within the cognitive dimension. Thus the IO doctrine of the Army, and to some degree the Marine Corps, was formed more completely with all three dimensions in mind. Still, despite encompassing all dimensions, the Army and Marine Corps doctrine was immature and failed to provide the momentum and organizational changes to fully integrate IO with its traditional operations.

The disparity between the services' understanding of IO generated significant challenges to integration of IO effects as the armed forces struggled to become increasingly "joint" in the late 1990s. This disparity became even more prevalent in the post 9-11 operations of Operation Enduring Freedom, prompting the Department of Defense to take significant measures to bridge

---

[27]U.S. Marine Corp Warfighting Publication (MCWP) 3-36, *Information Operations*, February 2001.

14

the gaps between the services. The result was the IO Roadmap, which will be discussed in detail in the next section.

Catalyst for Change: The IO Roadmap

Realization of the disparate understanding of IO between the services gave the Department of Defense (DoD) the impetus to conduct fifteen independent studies to identify causation, provide recommended changes to settle the differences and provide a common direction for the future of IO. The result of these studies was the classified publication of the *DoD Information Operations Roadmap* in October 2003. Declassified in 2006, this document provided the direction to establish IO as a core military competency. This distinction effectively brought IO to a level of parity with air, ground, maritime and special operations, and ultimately provided the political and fiscal backing to begin instituting the necessary changes in policy, organizational structure, education and management of an IO officer career field.[28] It also aimed to re-establish a full-spectrum framework for the three critical IO functions of 1) deterrence and disruption of the enemy, 2) protection of our own plans and misdirection of the enemy's, and 3) control of the adversary's communication and protection of our own.[29] When properly employed, these three functions should have mutually supporting relationships and once integrated will create substantial impact on both human and automated decision making.[30] With the framework for adapting the change established, the document went on to establish several significant recommendations.

The first of these recommendations was to create a common understanding of IO among the services, combatant commands and agencies. This was accomplished by narrowing the scope

---

[28]U.S. Department of Defense, *Information Operations Road Map* (30 October 2003), 2-4.
[29]Ibid., 8.
[30]Christopher Lamb, "Information Operations as a Core Competency," *Joint Force Quarterly*, December 2004, Issue 36, 90.

of the original thirteen IO core capabilities down to five and establishing standardized definitions

for the remaining five core capabilities of EW, PSYOP, OPSEC, MILDEC and Computer

Network Operations (CNO).[31] The effect of this action would ideally shore up the dilution of the

IO capabilities that existed in the previous categorizations of JP 3-13.

Next, the IO Roadmap recommended the need to consolidate the ownership and

advocacy for IO responsibilities in order to begin achieving unity of effort. The Under Secretary

of Defense for Policy (USD-P) was tasked to oversee this consolidation and subsequently

assigned US Strategic Command (STRATCOM) the responsibility of IO coordination across

areas of responsibility (AOR) and functional boundaries.[32] Although this directive sought to

eliminate the stove piping of information and effort under the previous constructs, the edict was

constrained by the next recommendation in the IO Roadmap which ordered the delegation of

capabilities and authority to the individual combatant commanders (COCOMs).[33] With this

added authority, the COCOMs would be required to conduct significant coordination with

STRATCOM to maintain unity of effort and insure against information fratricide. To help

matters in coordination, STRATCOM also created a Joint Force Headquarters for IO headed by a

three-star general. This organization was intended to not only supplement ongoing operations but

also act as a supporting and sometimes as a supported commander.[34]

The IO Roadmap also highlighted the need to create a well trained and educated IO

workforce. The document made the case for many of the previous IO shortfalls, namely that the

increased technical requirements of many of the IO elements created a natural isolation between

each of the disciplines. The Roadmap directed the creation of the IO career force which included

---

[31]U.S. Department of Defense, *Information Operations Road Map,* 10-11.
[32]U.S. Department of Defense, Joint Publication 3-13, *Information Operations,* 6 February 2006,
xii.
[33]U.S. Department of Defense, *Information Operations Road Map,* 12.
[34]Lamb, 92.

billets for senior executive and flag officer leadership positions. Further, it directed the Joint Services Staff College to develop a standardized education curricula for mid and senior career level officers.[35] Although the process of building this career force is still underway, this directive will soon provide a capable group of specialists who understand each of the five core capabilities and can properly advise commanders and integrate the three IO functions the into plans and operations.

The IO Roadmap made several other recommendations to achieve the status of IO as a core capability. Among them was the development of a long-term defense in depth strategy for Computer Network Defense (CND) and a need to mature Computer Network Attack (CNA) into a reliable warfighting capability.[36] This strategy centered itself on the premise of the DoD "fighting the net" almost as it would fight combat systems in the three dimensional landscape. Inherently important for this concept is the capability to maintain situational awareness, characterize, attribute, and respond quickly to attacks.[37]

Also included in the list of needed improvements to achieve the status of core competency was the initiative to increase PSYOP capabilities and support for our forces. Operation Iraqi Freedom highlighted some shortcomings in the PSYOP capabilities; namely that limited personnel and assets had trouble keeping up with the pace of operations on the way to Baghdad, and units were not getting the tailored messages needed to achieve the desired effect as they conducted their attacks.[38] Among the recommended improvements directed to help alleviate these deficiencies was the creation of a Joint PSYOP Support Element from Special Operations Command (SOCOM) intended to facilitate the coordination of products and programs between the combatant commanders and the Office of the Secretary of Defense (OSD). Further, SOCOM

---

[35]U.S. Department of Defense, *Information Operations Road Map,* 12.
[36]Ibid., 14-15.
[37]Ibid.
[38]Lamb, 95.

would continue with ongoing modernization efforts to develop increased technological capabilities and delivery systems.[39] Together, these recommended improvements should provide the maneuver commanders with much more responsive and flexible PSYOP support to their operations.

Finally, the IO Roadmap provided some direction to clarify and improve the distinction between PSYOP, Public Affairs (PA) and Public Diplomacy (PD). This is a topic which had been source of some controversy for our forces and had also limited our ability to target specific foreign audiences, so more clearly delineated direction was required. A brief review will shed light to the difficulties surrounding this topic.

Public Affairs are defined as public information, command information, and community relations activities directed toward both external and internal audiences with interest in DoD.[40] Meanwhile, Public Diplomacy exclusively targets foreign audiences and "includes those overt international information activities of the US Government (USG) designed to promote US foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers and by broadening the dialogue between American citizens and institutions and their counterparts abroad."[41] This distinction between PA and PD is regulated by the Smith-Mundt Act of 1948 which limits the characterization of information (specifically propaganda) which can be legally directed at US audiences.[42] Because the core IO element of PSYOP and related activities of PA and PD are restricted by law from providing false or aggrandized information to the American public, dynamics of the current global information environment create a tenuous situation.

---

[39] U.S. Department of Defense, *Information Operations Road Map,* 30 October 2003, 15.
[40] Joint Publication 3-13, II-8.
[41] Ibid., II-10.
[42] Public Law 402, "The US Information and Educational Exchange Act of 1948," 27 January 1948. Also referred to as the Smith-Mundt Act.

Recent dynamic changes in the capabilities of the world wide media and the internet have significantly blurred these legal lines. With the interconnectedness provided by the internet today, it is almost a foregone conclusion that information provided for foreign consumption will eventually reach the front pages of major newspapers, cable news broadcasts and websites. In order to avoid the possible pitfalls associated with unsynchronized PSYOP or PD messages reaching domestic audiences, the IO Roadmap's recommendations are critically important.

Thus the Roadmap established three recommendations to distinguish the individual roles of each function while also providing the guidance to ensure each function's efforts are mutually supportive and not conflicting or prone to information fratricide. The first recommendation directed that PSYOP would focus solely on support to military endeavors in environments where adversaries are present.[43] This measure ensures that the PSYOP messages are properly and precisely targeted, making it much more difficult for the message to be misconstrued if consumed by other than the target audience.

The second recommendation directed that DoD should collaborate with other agencies for PD programs and allow PSYOP to support the PD efforts.[44] Intended to help protect against information fratricide, this measure is intended to ensure that PSYOP messages crafted for use at the operational and tactical levels of warfare are properly nested with strategic messages and inter-agency efforts. The final recommendation relative to PSYOP, PA and PD suggests that PA efforts should be more proactive in its support of the USG PD objectives to include a broader set of select foreign media and audiences.[45]

Having reviewed the many recommendations of the IO Roadmap, it is clear that this document has provided the building blocks necessary to allow IO to become a core competency

---

[43]Department of Defense IO Roadmap, 16.
[44]Ibid.
[45]Ibid.

within the armed forces. Many of the recommendations are underway and will continue to evolve the transformation of our forces as we continue to adapt and engage our adversaries. Among the significant developments was the publishing of the updated Joint Publication 3-13 in February 2006. This publication, noted several times earlier in this paper, has adopted the necessary language to bridge the perceived gaps in the IO lexicon between the services. What remains to be seen is how well each of the services adapts to the recently modified framework of the joint publication. At the current time, each of the services is working on the development of their own updated IO doctrine consistent with the latest joint doctrine. As the services publish their new IO doctrine, we should finally begin to see the significant impact the IO Roadmap has had on the integration of IO and the ability of the joint community to think in terms of both the physical informational and cognitive dimensions of IO.

The next section will begin to examine the dynamics of integrating both the physical and mental aspects of warfighting in our current operations. An initial look into the theory of IO with respect to our heavily kinetic mindset will set the stage for the discussion of the integration of IO in the new Army and Marine Corps counterinsurgency doctrine.

CHAPTER THREE
CLAUSEWITZ AND IO: BALANCING THE PHYSICAL AND MORAL

The previous chapter highlighted the current state of IO within the joint community and

among the individual services. While some of the issues surrounding IO have been associated

with the lack of common understanding between the services, there is another element which has

hindered the effectiveness of IO as an effect on the battlefield. This element is the

misunderstanding of the relationship between IO and the more kinetically driven conventional

operations. This is not to say that IO should be considered as an unconventional element, rather

that IO needs to be thought of more conventionally in the framework of military operations and

should have a supported or supporting role depending upon the level of violence associated with

the type or phase of the conflict.[46]

This hypothesis has been described in detail in Colonel William Darley's noteworthy

article, "Clausewitz's Theory of War and Information Operations," published in the first quarter

2006 issue of Joint Forces Quarterly. This article analyzes IO in the context of Clausewitz's

theory of war and provides a practical model for how IO relates to kinetic operations across the

spectrum of conflict.[47] A detailed discussion of this premise and model will provide the proper

context for further discussion of current operations.

Darley began this discussion by reinforcing the principle that Clausewitz's theory was

intended to describe war holistically, both war's characteristics and its relationship with external

influences. Pivotal to Clausewitz's theory was his characterization of war as a political contest,

as seen in his famous passage "war is...a continuation of political intercourse, carried on by other

---

[46]William Darley, Colonel, US Army, "Clausewitz's Theory of War and Information Operations," *Joint Force Quarterly*, iss 40, 1st Quarter 2006, 73-79.
[47]Ibid, 74.

means."[48] Darley further established that war as a political conflict is dominated by two factors, violence and the moral or psychological. With these two factors transposed from violence and moral to the contemporary classification of kinetic operations and IO, one can propose that IO, as a subcategory of war, is an inherently political activity.[49]

Thus IO and kinetic operations share the purpose of achieving political objectives, however it is the context from which those objectives are interpreted that shapes the nature of the struggle. Too often, the military culture tends to maintain its focus on the kinetic factors, considering the rhetorical non-kinetic factors only as a supplementary effort. This is partly due to the ease at which the military culture can envision and arrange the tools for kinetic operations and the difficulty it has had in defining the purpose and use of the elements of IO as demonstrated in chapter two.[50]

The other factor which influences the military's focus on kinetic rather than IO is the level of violence associated with the conflict. The more violent the conflict becomes the closer it is to Clausewitz's ideal or "total war", and the less impact politics will have on the outcome. Conversely, the less violent the conflict, the more purely political it remains, and the less important the kinetic elements of the military framework are to the outcome.[51] Thus, as a conflict becomes less violent, the more dependent it also becomes on the non-kinetic elements such as IO to reach the political objectives. Darley illustrated this line of logic using a Clausewitzian continuum of violence with total war and pure violence at one extreme and pure politics with no violence at the other. (See Figure 1).

[48]Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87.
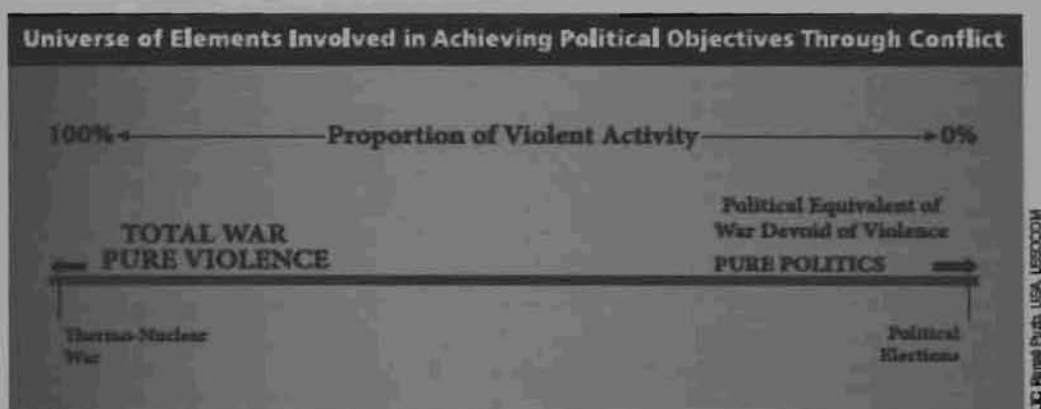[49]Darley, 74.
[50]Ibid.
[51]Ibid., 75.

Figure 1. Proportion of Violent Activity[52]

As shown this model presents real-world examples of events nearing or existing within

the two extremes. At the total war extreme, thermonuclear war resembles Clausewitz's notion of

pure violence and the near dissolution of political intercourse, while on the other end of the

continuum, the combination of rhetoric and the absence of violence during elections within stable

democratic societies illustrate the extreme of pure politics.[53] This examination of the two

extremes also led to Darley's contention that Clausewitz saw the need to make a distinction

between the politics within which war operates and the politics of diplomatic dealings.[54] This is

represented by the following quote from *On War*:

> While policy is apparently effaced in the one kind of war and yet is strongly
> evident in the other, both kinds are equally political. If the state is thought of as a person,
> and policy as the product of its brain, then among the contingencies for which the state
> must be prepared is a war in which every element calls for policy to be eclipsed by
> violence. Only if politics is regarded not as resulting from a just appreciation of affairs,
> but – as it conventionally is – as cautious, devious, even dishonest, shying away from
> force, could the second type of war appear to be more "political" than the first.[55]

---

[52]Ibid., 76. Figure 1 further attributed to LTC Renee Puzio, USA, USSOCOM.
[53]Ibid., 76.
[54]Ibid.
[55]Clausewitz, 88.

23

Using this distinction of two different forms of politics, Darley established an interim conclusion that "IO in its most extreme form would be a manifestation of pure politics," and further concluded that IO is not only a medium to communicate and influence policy but a participant in policy formation throughout the spectrum of conflict whose role increases as the conflict approaches the "pure politics" end of the continuum.[56] This distinction is critically important to the development of Darley's theory as it further reinforces the importance of IO within any conflict regardless of its position on the spectrum of violence. Further, it introduces the idea that IO plays a significant role in policy formation and development.

In the next step of the development of Darley's theory, he provided an explanation for what occurs between the two extremes. Using the previous model (Figure 1), Darley formulated the pattern for his final conclusion by arranging the examples of past conflicts along the continuum. Although Darley has arranged the conflicts in an admittedly subjective manner, they do reflect a rather logical order.[57] What is important from this model is not the exact order of the conflicts on the continuum, but rather the patterns that emerge from the illustration (See Figure 2).

From these patterns, Darley is able to arrive at some firm conclusions. First, that those conflicts which approach Clausewitz's total war construct have tended to achieve their political objectives through dominance of the physical dimension, be it geographically based, or the destruction of the enemy's forces. Conversely, those conflicts approaching the purely political side of the spectrum attained their political objectives through the dominance of the psychological

---

[56]Darley, 77.
[57]Ibid.

or moral dimension, or through influence and shaping of the public or adversarial decision maker's opinions.[58]
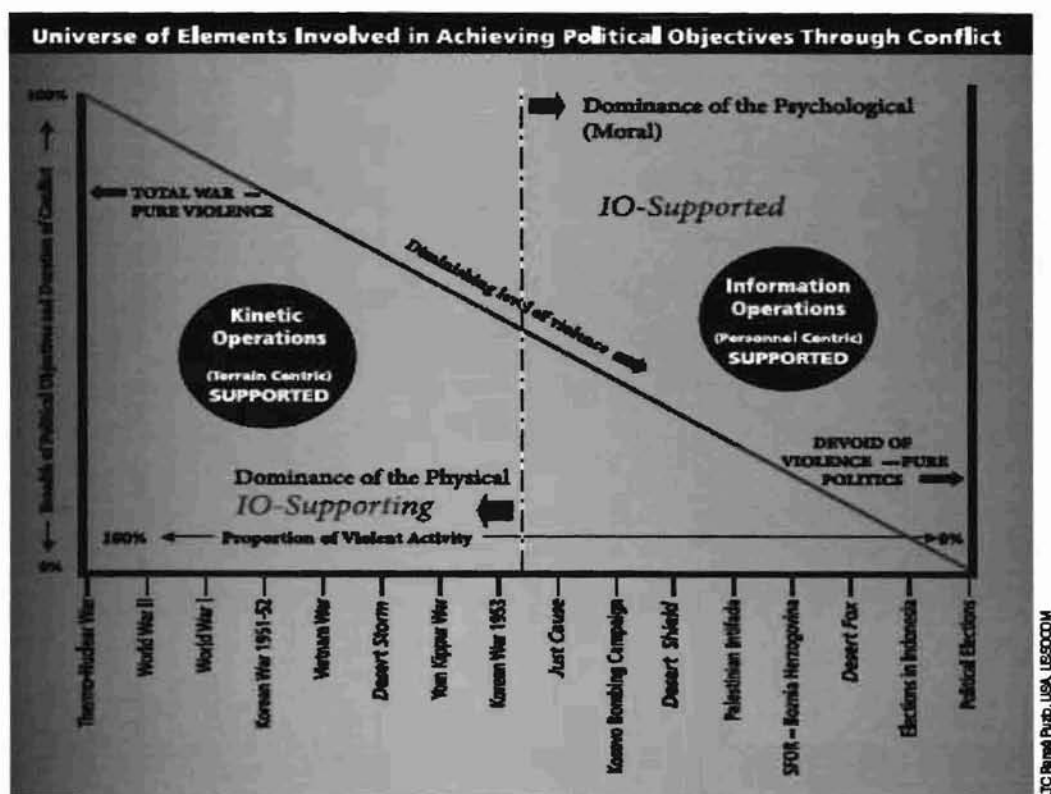

Figure 2. Political Objectives Through Conflict [59]

Darley suggests further that the dominance of either the physical or the psychological dimensions determines the role of IO as a supporting or supported effort. Existing somewhere in-between the two extremes is a threshold where that role shifts between kinetic and IO dominance.[60] This threshold is displayed as the center line on the illustration of Figure 2. It is important to note that while Figure 2 categorizes each individual conflict at a specific position on

---

[58]Ibid.
[59]Ibid., 78.
[60]Ibid.

25

however, the field is still significantly understrength and does not project being able to fulfill all of its manning requirements until 2013.[61] With these shortages, it will be some time before this corps of IO experts can create a lasting effect in their staff advisory roles in both combat and training.

Another significant education need is within the junior and mid-career officer service schools and branch specific advanced courses. At the time of this publication, the US Army Command and General Staff College (CGSC) does not provide a dedicated core curriculum block of instruction on IO beyond a single hour of instruction.[62] This situation is consistent with most of the US Army Officer Advanced Courses, with the lone exception being the Field Artillery Advanced Course. Upon graduation, the officers from these schools will prevalently assume positions within the maneuver battalion and brigade staffs of the Army. If the role of IO is to be understood and effectively integrated, it is essential that a basic understanding of IO exists beyond the FA 30 officer in the brigade headquarters.

---

[61] Joseph L. Cox, "Information Operations in Operations Enduring Freedom and Iraqi Freedom— What Went Wrong?" (Monograph, School of Advanced Military Studies, USACGSC, Fort Leavenworth, KS, AY 05-06), 26.

[62] Comments provided by the author's own records of core curriculum at the US Army Command and General Staff College during academic year 05-06 and corroborated by several students attending the 06-07 academic year.

Specific attention is needed at the battalion level as well. Although each of the maneuver brigades is allocated an FA 30 IO officer, there is no equivalent dedicated staff capability at the battalion level. The IO requirements at the battalion level generally fall upon the battalion Fire Support Officer (FSO) who maintains the responsibility for coordinating all lethal and non-lethal fires and effects. Because this individual is generally the only officer with any formal education in IO, he is often regarded as the single subject matter expert. Depending on this officer's proficiency, he may or may not have the requisite influence with the battalion's commander to elevate IO to its required level of importance within COIN operations. If he is not capable of this influence, a field grade or even company grade officer with a basic understanding of IO principles could provide the necessary support.

This potential deficiency highlights the need for some form of formal IO education across all branches at the junior and mid-career officer's courses. Until the education and training catches up with the requirements in operational and tactical units, it is critical that policy makers and military commanders begin to understand this link between IO and kinetic operations and can properly recognize and refine the specific political objectives of the conflict to determine if it is predominately kinetic or informational in nature.[63]

It is also important that commanders and policy makers continually conduct these assessments throughout the conflict. As mentioned earlier, conflicts will experience transitions through different phases throughout its life cycle. Even mature conflicts that have transitioned through the threshold from kinetic to IO are capable of regressing back towards a more kinetic nature. An excellent example of this regression in Iraq occurred following the destruction of the Al-Askari Mosque of Samarra in February 2006. The sectarian violence which followed radically

---

[63]Cox, 79.

changed the dynamics within Iraq's immature political structure and required the re-assessment of our own political objectives and the nature of the war itself.

The exploration of IO doctrine and the theoretical relationship between IO and kinetic operations has set the conditions to begin an evaluation of IO within current operations. As US and coalition forces are fully engaged in the counterinsurgencies of Iraq and Afghanistan, the evaluation will begin with a review of the role of IO as proscribed in the Army and Marine Corps' new field manual for COIN operations, FM 3-24.

CHAPTER FOUR
COUNTERINSURGENCY DOCTRINE AND THE ROLE OF IO

In the months following the fall of Baghdad in April 2003, the United States military was faced with the stark reality of a new dynamic. Namely, that for the foreseeable future it is unlikely that the United States would face a conventional military threat that would stand up to fight in a major, inter-state combat operation.[64] While some potential peer competitors could threaten the United States conventionally in the long term, most potential adversaries observed US operations against the Taliban in Afghanistan and against Saddam's Iraqi Army and recognized that a Fabian strategy of exhaustion is much more efficient and effective than one of annihilation against the existing conventional overmatch.[65]

As coalition forces in Iraq struggled to first recognize and then adapt to the rising insurgency on the ground, the US forces, schools and Combat Training Centers (CTCs) at home began their own preparations for what would eventually be recognized as COIN operations. As these preparations began however, existing Army doctrine for COIN operations consisted of little more than a four-page section from the February 2003 Army publication, FM 3-07, *Stability Operations, and Support Operations (SOSO)*. Units preparing to deploy were thus required to search through superseded doctrine such as the 1990 publication, FM 100-20, *Low Intensity Conflict*, or the *Marine Corps Small Wars Manual*, which was first published in 1940. Many

---

[64]LTC John Nagl and LTC Paul Yingling, "New Rules for New Enemies" *Armed Forces Journal*, October 2006, 25.
[65]Ibid.

even explored authors such as Sir Robert Thompson, T. E. Lawrence, and Roger Trinquier to find insights and methodologies for fighting an insurgency.[666768]

The October 2004 publication of Interim Field Manual (FMI) 3-07.22 *Counterinsurgency Operations* provided relief for this deficiency. Still, this interim manual simply served as an "expedited means to provide a fusion of doctrine and tactics, techniques and procedures (TTPs) to the force."[69] With a two-year expiration date, the manual was scheduled to be superseded in October 2006 by the new doctrinal manual FM 3-24.

FM 3-24 – A Solid Base for Counterinsurgency Operations

FM 3-24 *Counterinsurgency*, also titled Marine Corps Warfighting Publication (MCPW) 3-33.5, was released on 15 December 2006. With a great deal of anticipation, the new manual finally provided our forces with the framework for COIN operations which had been absent since the end of the Vietnam War. The manual was released amid significant media attention and in conjunction with the President's new strategy for Iraq. Despite the attention and the proximity of its release to the new grand strategy, FM 3-24 did not claim to be the all-knowing book of answers or that it would provide the elusive silver bullet that would solve the military's problems in Iraq or Afghanistan. Instead, the manual was appropriately prefaced with the disclaimer that "it is not intended to be a stand alone reference", and that "it is based on existing interim doctrine and doctrine recently developed"[70]. This disclaimer correctly suggests that this manual is not necessarily a complete how-to reference on COIN and that continual assessment, review and

---

[66]Sir Robert Thompson authored *Defeating Communist Insurgency; The Lessons of Malaya and Vietnam* in 1966. He is regarded as a counterinsurgency expert and is acknowledged as such in the preface of FM 3-24.
[67]T. E. Lawrence authored *The Seven Pillars of Wisdom* as an account of his experiences in the Arab revolt from 1916-1919.
[68]Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (London and Dunmow: Pall Mall Press, 1961), translated by Daniel Lee.
[69]Interim Field Manual 3-07.22, *Counterinsurgency Operations.*
[70]U.S. Army Field Manual 3-24, *Counterinsurgency*, 15 December 2006, vii.

refinement is necessary to maintain relevance on the subject. Despite these disclaimers, FM 3-24 is a superb source of information, reference and tools, and provides our forces with excellent examples of COIN approaches and methodologies.

FM 3-24 states that its target audience is "leaders and planners at the battalion level and above," yet it is a valuable reference for leaders at all echelons from the squad up to the strategic levels.[71] The manual provides strategic and operational context through the use of many vignettes from both history and recent events. Beyond the vignettes, FM 3-24 also provides relevant strategic and operational discussions in chapters dedicated to the principles of unity of effort and campaign design. The first of these chapters focuses on achieving unity of effort through the integration of the various civilian and military organizations across all levels of war.[72] Meanwhile the chapter discussing campaign and operational design provides considerations for command and control doctrine and planning doctrine as it applies to the planning a COIN campaign.[73] Despite these forays into the strategic and operational levels of war, the remainder of the manual remains heavily weighted towards the tactical level. It appears the manual's principle focus is to provide tactical leaders and planners with the framework and principles required to plan and execute COIN operations.

FM 3-24 begins with a contextual overview of insurgency and counterinsurgency, which in general, reads much like an introductory history lesson on insurgency and COIN. The first section of the chapter presents many historical examples of insurgencies, providing the background, framework, dynamics and vulnerabilities encountered in several past conflicts. This section includes a broad range of examples, from the current religiously fueled conflict, to Mao Zedong's political ideology based insurgency to the criminally based activities of the Fuerzas

---

[71]Ibid., vii.
[72]Ibid., Chapter Two.
[73]Ibid., Chapter Four.

Armadas Revolucionarias de Colombia or FARC.[74] This historical context accomplishes two purposes. First, it provides the reader excellent perspective on the many variants of insurgencies, and reinforces appreciation for their complexity and adaptability. Second, the historical context also prepares the reader for chapter three's discussion of intelligence in COIN and the significant importance of looking at the sources of conflict holistically in order to understand the cultural, ideological, religious and socio-economic issues and their impact on the operational environment.

As the first chapter transitions from descriptions of insurgency to COIN, the character of the narrative also transitions from descriptive to more of a directive tone. Although still historically rooted, the section begins with a brief discussion of the full-spectrum requirements of COIN before presenting some principles and imperatives for execution of COIN operations. Through the discussion the reader is reminded that these principles are historical examples of past counterinsurgencies and may or may not apply depending on the circumstances and adaptations of the existing conflict. The review of these historical principles essentially establishes the outline for the remainder of the manual.

Perhaps one of the most interesting narratives in the manual is the discussion of the many paradoxes of COIN, found at the conclusion of the first chapter. This discussion on paradoxes highlights the imperative that within COIN operations, conventional thoughts on conflict must be substituted by a more expansive and agile mindset.[75] The traditional set of considerations for missions and procedures may not necessarily apply. The excerpts "sometimes the more force is used, the less effective it is," and "some of the best weapons for counterinsurgents do not shoot" are both excellent examples of the unconventional mindset required in the COIN environment.[76]

Although the manual is heavily reliant upon historical conflicts to present its examples for its framework, it stresses the need for coalition forces to maintain agility and the ability to

---

[74]FM 3-24, 1-10-12.
[75]Ibid., 1-26.

assess and adapt to the unique conditions they encounter within their areas of responsibility. This concept of agility is continued within the framework the manual prescribes in its chapter on campaign design. Chapter four of FM 3-24 states that while COIN campaigns are centralized in design at the strategic and operational level, the campaign's execution is decentralized in nature and should truly be controlled at the company level and below. Within this framework, initiative is an absolute necessity and should be enabled at the lowest levels in order to assess and shape the policies, tactics and procedures appropriate for each localized area of operations.[77] As the individual commanders shape and adapt their operations for their own localized areas, it is imperative that each commander maintains a continuous dialogue vertically across echelons as well as horizontally across the battlespace. Continuous coordination should ensure that all commanders understand the causal relationships between friendly actions and the insurgent's adaptations.[78] Further, this coordination will allow for the senior commander to continually assess and modify the direction of the campaign design to ensure unity of effort and progress toward the political objectives.

There are two other themes which were given significant attention throughout the manual. The first of these themes was the importance of politics and political power. The manual clearly establishes in the first few paragraphs that political power is the central issue for both the insurgent and the counterinsurgent regardless of the underlying causes for the conflict. Despite the occasional presence of an apolitical group or criminal element within the struggle, ultimately what insurgents are trying to achieve is legitimacy for their cause or organization and establish the illegitimacy of the existing political entity. The importance the manual associated with the need for both sides of the conflict to gain political power and establish legitimacy to

---

[76]Ibid.
[77]Ibid., 4-3, 4-4.
[78]Ibid., 4-6.

achieve success in the campaign is consistent with Clausewitz's theory of war as a political

struggle. Recalling back to the dialogue in chapter three of this paper, this line of thought is also

consistent with Darley's theory on the relationship between kinetic and IO efforts, and the need to

balance these elements in order to achieve the political objectives.

The second theme found throughout the COIN manual is the importance of IO and the

absolute necessity of its integration into the operational framework of the campaign. IO is given

significant attention in the dialogue provided in chapter five – Executing Counterinsurgency

Operations.

IO and COIN Doctrine

With the frequency that IO is mentioned throughout the manual, it is clear that FM 3-24

recognized the importance of IO in COIN operations. The discussion of Darley's theory in

chapter three establishes that IO's relative importance within COIN is largely attributable to the

political nature of these types of conflicts.[79] FM 3-24 appears to concur with Darley's theory.

The importance that FM 3-24 places on the struggle for political legitimacy for both insurgents

and counterinsurgents implies that these types of conflicts will be fought well beyond the physical

dimension and into the cognitive dimension of the information environment as all sides of the

conflict compete for public support of their political objectives. Thus within the framework that

FM 3-24 presents, IO is an element of critical significance to the political outcome of these

struggles.

FM 3-24 begins to establish the struggle within the cognitive dimension in its description

of insurgencies and the information environment in chapter one, however, the topic truly gains

momentum in chapter three's evaluation of the threat's use of information and the media.[80]

---

[79]Darley, 78.
[80]FM 3-24, 3-17.

Chapter three's discussion establishes the argument that insurgent information and media activities may in fact be the main effort to undermine the legitimacy of the ruling government and generate public support for their cause.[81] By using every form of media available, insurgents effectively highlight their own successes as well as the failures and missteps of the host nation or COIN forces. A key advantage for the insurgent is that their messages do not necessarily need to be based on factual information to be successful. Instead, the insurgent's messages must only briefly resonate with the targeted public to create the skepticism about the legitimacy of the government's cause in order to create its desired effect.[82] Examples of this phenomenon can be seen throughout contemporary operations in Iraq and Afghanistan and will be discussed in greater detail during the discussion of the current information environment.

FM 3-24 again pays significant attention to the role of IO in its chapter on execution of COIN operations. As the chapter explores logical lines of operation (LLOs) as a means for commanders to visualize, describe and direct their operations in COIN operations, IO is visually represented in three graphic models as an element which encompasses all LLOs. Although these graphics are simply examples of past commander's operational models, it is significant to note their perceived relationship within the context of the other operational lines (see Figure 3). This particular example demonstrates that while IO is itself an LLO, it is also critical that the elements of IO are incorporated within each of the other LLOs to help influence the population's perceptions of the LLOs' success.
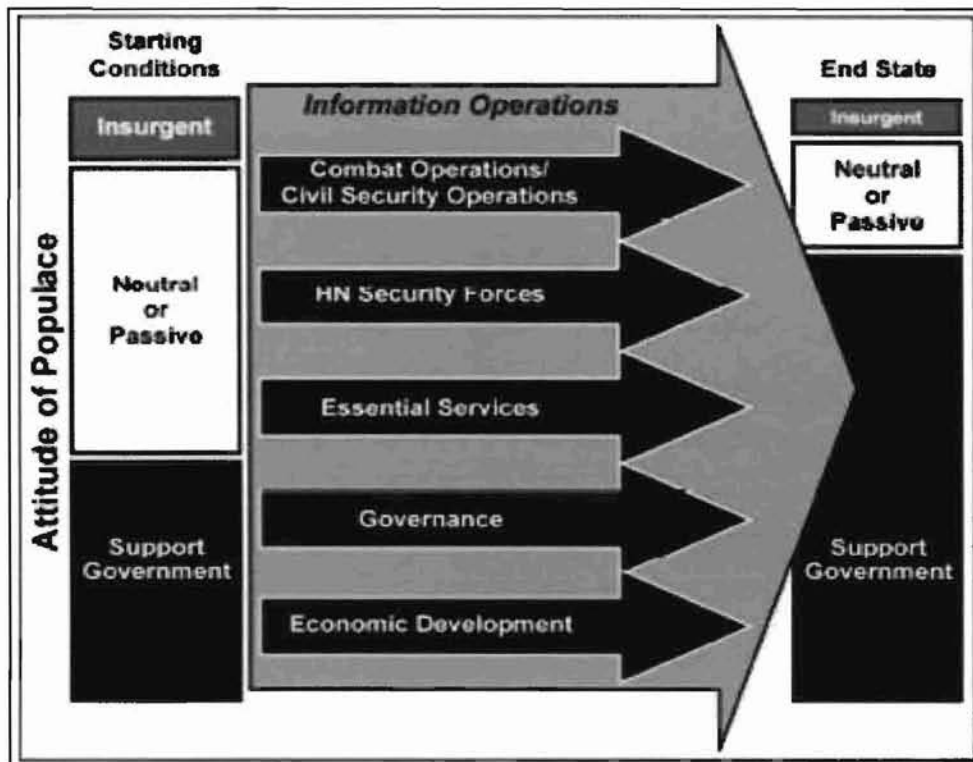
---

[81]Ibid., 3-17.
[82]Ibid.

Figure 3. Example COIN Logical Lines of Operations[83]

FM 3-24 provides descriptions of each of the individual LLOs, the first of which is the

conduct of IO. In this section, the manual highlights many of the tasks and IO considerations the

command must accomplish in order to properly integrate and synchronize the efforts of all other

LLOs. Among these necessary tasks is the need to manage the public's expectations, sustain the

unity of the message across all echelons of the command, and reinforce the validity of the themes

and messages through consistent, firm, fair and professional actions of the Soldiers and Marines

on the ground.[84] This section continues with an extensive list of considerations for the integration

of the IO LLO, and concludes with dialogue which reinforces the commander's need to take an

---

[83]Ibid., 5-4, thru 6, Figures 5-1, 5-2 and 5-3 of FM 3-24 each provide graphic representation of IO as an element which encompasses all other LLOs. The figure represented here is figure 5-1 from the manual.

[84]Ibid., 5-8.

active role in shaping the military's relationship with the media. Such considerations include guidelines for the treatment and inclusion of embedded reporters within the individual units.[85]

In chapter five, FM 3-24 provides three different approaches to the application of COIN principles. The operational approaches provided in this section of the chapter include the Clear-Hold-Build, Combined Action, and Limited Support methods.[86] In this discussion, the manual describes the target audiences as well as the potential themes and messages the force might wish to employ consistent with each phase of the operation. Again the manual predicates these recommendations as simply examples from which the user should adapt and/or combine to meet the specific needs of their individual conflict.[87]

Despite the significant attention FM 3-24 allots to the role of IO in COIN, the content of the dialogue is unquestionably incomplete. The entire focus of the manual's discussion of the IO LLO is on the elements, supporting elements and related activities of IO which both primarily relate to the cognitive dimension and also are broadcast to the general public. Such elements include PSYOP, PA and Military Support to Public Diplomacy. Completely absent from the discussion are the primary IO elements of MILDEC, OPSEC, EW, and CNO. FM 3-24 acknowledges that its dialogue does not address the full palette of IO elements in its discussion of the IO LLO.[88] Despite this disclaimer, this omission is indicative of some of the issues which still exist in the IO realm. Namely, that the Army and Marine Corps are continuing to develop its IO specialties in directions inconsistent with the directives of joint doctrine.

Some of these omissions can be explained logically. For instance, OPSEC and MILDEC are related in their purpose to undermine our adversary's understanding of our operations. MILDEC consists of actions taken to deliberately mislead adversary decision makers as to

---

[85]Ibid., 5-9, thru 11.
[86]Ibid., 5-18 thru 25 provides a detailed description of each of the three COIN approaches.
[87]Ibid., 5-18.
[88]Ibid., 5-9.

friendly military capabilities, intentions, and operations in order to create false assumptions and lead the adversary towards a course of action less capable of countering friendly operations.[89] Meanwhile OPSEC consists of actions taken to protect friendly operational information from even reaching the adversarial commander.[90] While both elements are important, they are also both fundamentally part of normal operations, much like physical security is a fundamental part of operations. It is not unreasonable to assume OPSEC and MILDEC will be incorporated into the COIN operational design.

Still, there is no indication in FM 3-24 that the Army is pursuing the integration of EW or CNO into its COIN operations as neither of these primary IO elements receive any attention within the manual. Perhaps this is due to the target audience of the manual being predominately tactical, and the extremely limited EW and CNO assets tactical commanders have directly under their control. Yet since neither the Army nor Marine Corps have yet published an updated IO doctrine since the release of JP 3-13 this conclusion is entirely speculative. However, the dialogue presented in FM 3-24 suggests that Army and Marine Corps no longer hold the elements pertaining to the electronic spectrum as a significant priority in the COIN information environment.

Despite these omissions of primary IO elements, FM 3-24 provides a valuable framework for US and coalition forces as they prepare and execute COIN operations in the contemporary environment. The manual's focus on politics as a central issue in the conflict and the subsequent importance it attributes to IO appears to be consistent with the requirements of our contemporary global information environment. Still there are dissenting views. Detractors of the new COIN manual such as Ralph Peters, a retired US Army officer and frequent critical commentator, argue that the manual is entirely too "touchy feely" and that the authors' choice of historical examples

---

[89]Joint Pub 3-13, II-2.
[90]Ibid.

selectively omitted those conflicts where overwhelming, indiscriminate force and the ruthless measures against detainees and the public were the decisive elements to the conflicts' success, not the soft-power of IO and its related activities.[91] Although Peters presents an interesting argument for the use of extreme measures in COIN operations, his conclusions fail to acknowledge the realities of the impact of the global information environment and politics of today. As the exposure of events such as the Abu Gharaib prison scandal have demonstrated, the world will be both witness to and a judge of the methods used in contemporary conflict, and the US cannot simply abuse its position in the world to try and find a quick or easy solution to the difficulties it currently faces.

The reality of today's global stage is just one of many aspects of the operational environment that US forces must understand in order to effectively integrate IO into the overall operational design. Fully understanding the relationship of the information environment within the contemporary operational environment is necessary to provide the context for the many considerations needed to effectively employ IO in current operations.

---

[91]Ralph Peters, "Progress and Peril: New Counterinsurgency Manual Cheats on History Exam," *Armed Forces Journal*, February 2007, 34-37.

CHAPTER FIVE
UNDERSTANDING THE CONTEMPORARY INFORMATION
ENVIRONMENT

The Army or Joint Forces Commander must understand that as a function of the

contemporary operating environment there are two primary realms, the physical areas and factors,

and the information environment.[92] Understanding the information environment and how it

relates to the physical realm of the operational environment is a key component to the effective

integration of IO into contemporary operations. JP 3-13 defined the information environment as

"the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act

on information."[93] More succinctly, "the information environment is where humans and

automated systems observe, orient, decide, and act upon information, and is therefore the

principal environment of decision making."[94]

As mentioned earlier, the information environment consists of three separate dimensions

which include the physical, informational and cognitive. The physical dimension is where the

information environment overlaps with the physical world and includes the command and control

systems and supporting infrastructures that enable individuals and organizations to conduct

operations in all four of the battlespace domains – air, land, sea and space.[95] The physical

dimension is where maneuver and combat operations occur, and for IO this is the dimension in

which information systems are attacked and defended.

The informational dimension is dual natured. It is both where the information is

communicated, stored, disseminated and displayed, and it is the message itself. This is where the

commander's intent is conveyed and it is where the information must be protected. It is the world

---

[92]Joint Pub 3-0, II-19.
[93]Joint Pub 3-13, I-1
[94]Ibid., I-1.
[95]Ibid., I-2.

of microchips, microwaves and cyberspace and it is the bridge between the physical and the cognitive dimensions.[96] In this dimension IO is focused on the content and flow of the information processes.

Finally, the cognitive dimension encompasses the mind of the decision maker and of the target audience. This is the dimension where people think, perceive, visualize, and decide and it is influenced by such intangibles as emotions, public opinion, the media, rumors, and situational awareness. As battles can be won and lost in the cognitive dimension, it is the most important of the three dimensions.[97] Collectively the three dimensions have an interrelationship and form the information environment.

While the information environment exists within the overarching operating environment, and exists within each of the physical domains – air, land, sea and space – it is still distinct from them. If looked at using a systems perspective, the relationships between the different dimensions of the operating environment are interconnected and have elements existing in more than one dimension. The graphic perspective of this relationship is shown in Figure 4.

Given these interconnected relationships, for every activity taking place within the physical environment, there is a simultaneous activity or effect occurring within the related information environment.[98] This has implications on commanders as they must attempt to gain a holistic understanding of the operating environment in order to properly visualize, describe, and direct their operations to create effects in both the physical and informational realms. In order to gain this understanding, commanders rely on the staff's conduct of the Intelligence Preparation of the Battlefield (IPB) or the Joint Intelligence Preparation of the Battlespace (JIPB) processes.

---

[96]Ibid.
[97]Ibid.
[98]Norman Emery, MAJ USA, "Fighting Terrorism and Insurgency: Shaping the Information Environment," *Military Review*, Jan-Feb 2005, 34.

THE INTERCONNECTED OPERATIONAL
ENVIRONMENT

Information

Social

Infrastructure

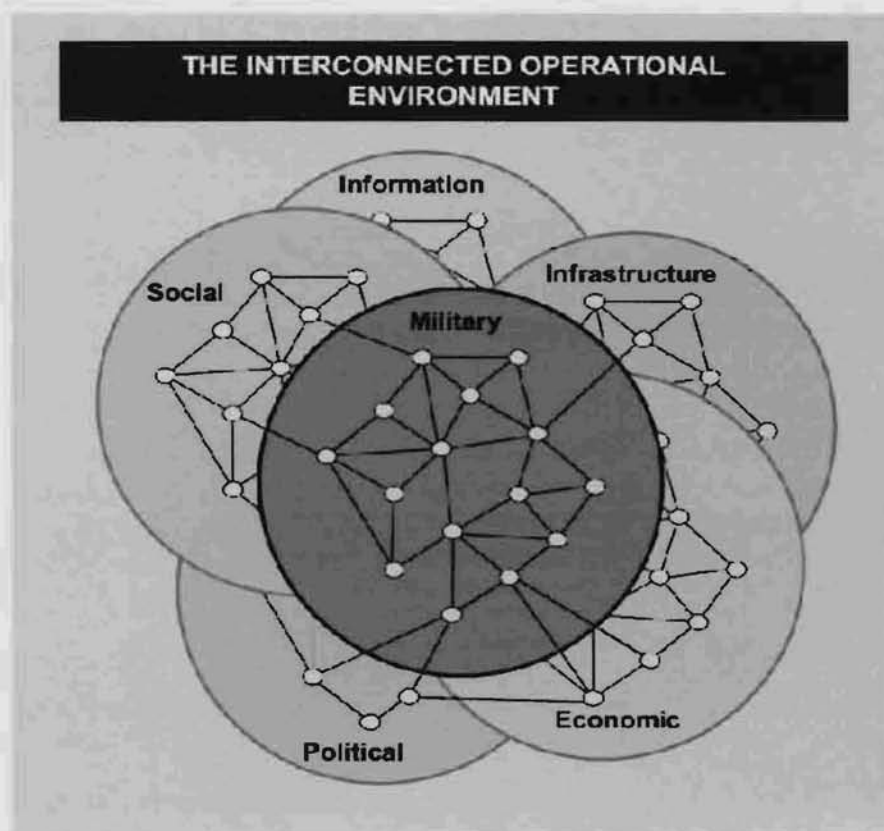Military

Economic

Political

Figure 4. The Interconnected Operational Environment. [99]

As the IPB or JIPB processes have traditionally focused on the threat and physical domains of the battlefield or battlespace environments, the relatively recent acknowledgement of the importance of the information domain requires a broader scope. The JIPB process must now include detailed studies of the effected society to include the culture, religious influences, societal demographics, history, political and economic factors in order to gain a holistic understanding and ensure proper integration of the IO efforts. Because of the expansive amount of information and expertise required for this additional requirement, the process is being aided by the Joint Forces Command (JFCOM) development of the Operational Net Assessment (ONA) concept.

---

[99]U.S. Army, Joint Publication 3-0, *Joint Operations*, Figure II-6, II-22.

The ONA concept aims to provide a collaborative network of analysis and information from various US and foreign government agencies to enhance our commanders' decision making capabilities.[100] This network is intended to be continuous and dynamic, and should provide updated information in wartime and peace so commands and planning staffs may reach-back for the knowledge required to gain comprehensive understanding of their operating environments.[101] This relatively new concept is still under development. Once the network is fully developed, truly collaborative, and made available to all operational units, it should prove to be a tremendous asset to units developing understanding of the information environment.

As a result of the expanded analysis and understanding of the information environment, the staff should be able to create a Combined IO Overlay to help the commanders visualize the complexity of the environment within their respective areas of operation (AO). This overlay is very similar to the Military Combined Obstacle Overlay (MCOO) which has long been used to help commanders and staffs visualize the terrain and analyze its effect on friendly and enemy operations. Instead of terrain, the IO overlay can incorporate a vast combination of demographical and threat overlays along with host-nation and coalition media capabilities to create a visual picture of the specific characteristics of the AO. This analysis ultimately enables the command to precisely identify and tailor the IO objectives to the specific populations. An example of a media overlay is provided in Figure 5.

---

[100]US JFCOM website provides a complete definition and explanation of the ONA concept. http://www.jfcom.mil/about/fact_ona.htm.
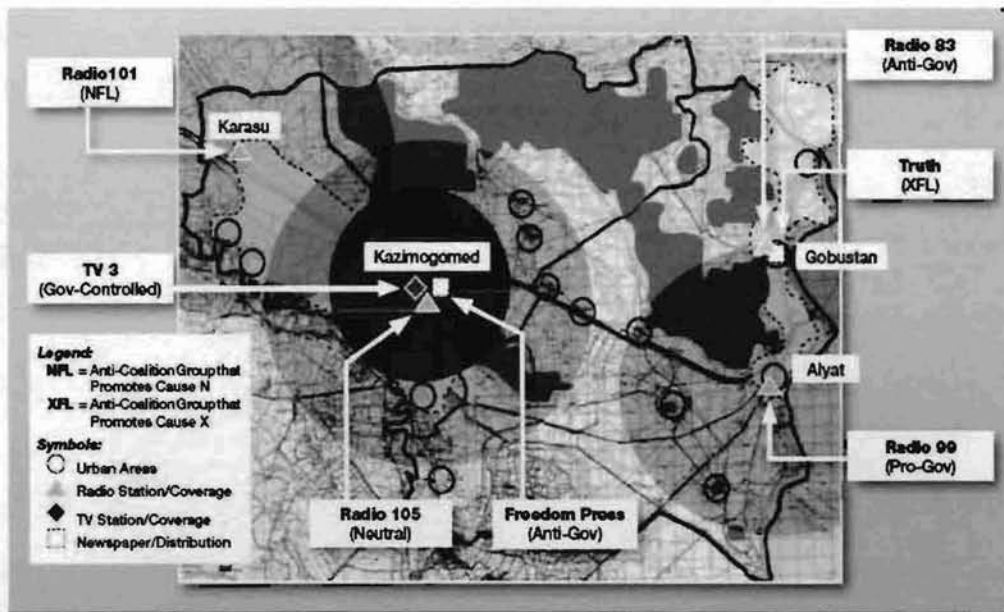[101]Ibid.

Figure 5. Combined IO Overlay for Media.[102]

In addition to understanding the information environment as it relates to the physical

environment, commanders also need the means to assess the effects of their IO and physical

efforts in order to adapt their operations to changing conditions of both the adversary and the

environment. This is yet another shortfall of the US doctrine as there is very little written about

assessment in general and most of what does exist pertains to Battle Damage Assessment (BDA)

within the lethal targeting process.[103] Further, most of the established assessment assets and

methods were devised to assess the immediate effects of lethal operations and are less proficient

at capturing the longer-term effects required to execute an IO campaign.

The means to capture the long-term effects of an IO campaign are through the

command's establishment of Measures of Effectiveness (MOE) and Measures of Performance

(MOP). Once again, while the function of MOEs and MOPs are described within doctrine, very

---

[102]Erin A. McDaniel and Julio A. Perez, "How to Visualize and Shape the Information Environment," *Field Artillery Magazine*, November-December 2006, 30.
[103]Cox., 20.

little guidance exists on their actual development.[104] Since MOPs deal in the assessment of the

effective delivery of the lethal or non-lethal methods their measurement is more concrete and

easier to develop. Conversely, MOEs are not as simple to construct, particularly when dealing

with the effectiveness of a non-lethal measure or IO message. These abstract measurements are

difficult to develop, manpower intensive to attain and analyze, and very susceptible to subjective

assessment. MOEs must also be established and interpreted within the context of the culture,

politics and socio-economics of the area of operations being measured. MOEs should be

developed with the following principles in mind. They should be observable, quantifiable, and as

precise as possible to insure they can be collected, and objectively assessed.[105] Their effective

development and interpretation is completely dependent upon how well the command

understands their operational and informational environments.

The success of MOEs and MOPs is also greatly dependent upon the command's ability to

collect and analyze the proper information. This process is manpower intensive and heavily

dependent upon the successful collation of traditional intelligence collection assets as well as

those assets and sensors from the IO field. The traditional Tactical Human Intelligence (TAC-

HUMINT) capabilities and units' tactical patrols feed reports and debrief information into the

standard intelligence channels, usually populating the databases on the All Source Analysis

System (ASAS) network. Meanwhile, the reports generated by Civil Affairs and PSYOP surveys

are routed through the IO cells of brigade and higher headquarters and are maintained in separate

database systems from the intelligence community. Because these IO and Military Intelligence

(MI) databases are maintained on separate and incompatible systems, intelligence analysts are

thus required to work with multiple databases or deliberately collaborate with the IO sections to

---

[104]Ibid., 21.
[105]David C. Grohoski, Steven M. Seybert, and Marc J. Romanych, "Measures of Effectiveness in the Information Environment," *Military Intelligence Professional Bulletin*, Jul-Sep 2003, 14.

gain complete understanding of the reported information.[106] This additional layer of coordination achieves a more completely understood assessment, but it also significantly affects the timeliness of the analysis, which may have a negative impact on the responsiveness and agility of the IO campaign.

Information Environment Considerations in COIN Operations

With the many considerations for understanding the information environment in mind, there has been considerable dialogue within professional publications and journals highlighting the experiences and lessons learned regarding the information environment and its relation to the COIN operations. One recent publication of great significance is the US Army War College Workshop Report, "Shifting Fire: Information Effects in Counterinsurgency and Stability Operations." This report was published following the 30 November, to 1 December 2005 workshop "Information Operations and Winning the Peace" at the Center for Strategic Leadership at Carlisle Barracks, Pennsylvania. The report captures the commentary from the sixty participants of varying professions, including the military, national security, intelligence and interagency communities, as they discussed case studies from 2002's second Intifada phase of the Israeli-Palestinian conflict. As the title suggests the discussion focused on the changing roles of IO in COIN and Security, Stabilization, and Reconstruction Operations (SSTRO).[107]

Several key and inter-related takeaways emerged from these discussions which, although taken within the context of the Israeli-Palestinian conflict, provide timeless information considerations for COIN operations both within the current conflicts and beyond. A brief review

---

[106]Cox, 23.
[107]Deirdre Collings and Rafel Rohozinski, "Shifting Fire: Information Effects in Counterinsurgency and Stability Operations," report from US Army War College workshop held 29 November – 1 December 2005, 29.

of these key takeaways will identify many of the considerations required in the global and COIN

information environments, and will reinforce many of the thoughts discussed earlier in this paper.

The first of the takeaways was framed within the perspective of the global environment.

This takeaway established that "no single actor can control the information sphere".[108] The

premise is that the global information environment is an open system, and it's available to anyone

with an internet connection, and the desire to engage a target audience with their message. With

today's availability of relatively inexpensive technology, the thought that the information

environment can be dominated or even controlled is now artificial. Instead of trying to control

the environment, we should focus our efforts on getting our information in front of the other

participants who are vying for influence.[109]

Shifting from the global environment, the report begins to focus on the considerations of

the information environment specifically within the COIN and SSTRO battlespace. Within this

section, the report establishes that the support or acquiescence of the population is the key to the

insurgent's capability to continue their struggle. Without the intelligence, logistics and safe-

haven provided by the population, the insurgency cannot sustain itself. Thus the center of gravity

(COG) in the COIN environment is the population, rather than the insurgent, and the primary

objective for the counterinsurgent is to attract and maintain the willing support of the people, thus

denying support to the insurgents.[110]

With the COG firmly established as the population itself, then the main form of "fires" in

the COIN/SSTRO environment is informational, not kinetic.[111] Predominately kinetic operations

will not convince the population or the insurgents that the host nation or counterinsurgent force's

ends, ways and means are legitimate. Instead, kinetic operations may provide additional support

---

[108]Ibid., 15.
[109]Ibid.
[110]Ibid., 16.
[111]Ibid.

and recruits to the insurgent's movement. Thus, information based operations focused on the political ends of legitimizing the host nation and discrediting the insurgent are the means to gain resonance of the host nation's cause.[112]

The insurgents fully understand this dynamic and maintain a marked advantage as they are organized to operate predominately in the informational and political realms. Although the insurgents use kinetic operations, their true objective is always to send a strategic message.[113] As stated earlier in chapter four, insurgent's messages do not necessarily need to maintain truth, they must simply resonate the illegitimacy of the host nation or the COIN forces. The insurgents further understand that the message that reaches the population first, regardless of its credibility, is often the message that maintains the momentum and resonation with the public.[114] It is critically important then, that COIN forces recognize the political nature and adapt their organization and operations accordingly. When kinetic operations are employed, COIN forces must consider the use of shaping IO both before and after the direct action in order to proactively manage the consequences of the operation and get ahead of insurgent attempts to undermine the COIN force's legitimacy.[115] Although previous US COIN doctrine failed to recognize the political and informational nature of COIN operations, the new manual FM 3-24 established this transition and leans heavily toward the political and informational aspects of operations.

COIN forces must also recognize that the military is not the only element of national power available to leverage in the informational struggle. As the conditions of the global information environment make the boundaries of strategic, operational and tactical levels of war more transparent, more thought must be dedicated to the coordination of the themes and messages

---

[112]Ibid.
[113]Ibid.
[114]Stephanie Kelly, "Rumors in Iraq: A Guide to Winning Hearts and Minds" (Thesis, Naval Post Graduate School, Monterey, CA, 2004), 6.
[115]Collings and Rohozinski, 17.

to ensure unity of effort.[116] Once again, FM 3-24 has acknowledged this necessity and dedicated an entire chapter to the integration of interagency and non-governmental organizations.

Of course, an effective strategy and unity of effort among all elements of national power is predicated on the establishment of a clearly defined and comprehensively understood end-state.[117] In order to gain and maintain legitimacy with the host nation's populace however, the end-state and strategic objectives must appeal to the population's interests and desires. The nation supporting the COIN effort must protect against the projection or mirror-imaging of their values and ideals when establishing the end-state.

The dangers of mirror-imaging go beyond establishing the desired end-state. COIN forces must attempt to fully understand the ways they are perceived by the local population in order to properly design their messages and maintain legitimacy of their efforts. Perceptions of occupation or colonization by the COIN forces, historical precedence of past actions by the nation supporting the COIN effort, or even existing relationships with neighboring countries may severely detract from the IO effort's ability to resonate with the population.[118]

Cultural expertise and situational understanding of local political and economic dynamics are also essential for the proper development of IO objectives.[119] Cultural expertise is not something that can be attained through pre-deployment training programs, and the US Army does not have the inherent expertise within its ranks. COIN forces must therefore have the capability to reach-back to utilize the knowledge of regional and country experts. Again, the ONA concept is working to develop that capability, however it is uncertain what echelon of command will have that asset at their disposal. Conversely, situational understanding can be developed from the interaction and engagement of the local population. This process will take time to truly gain

---

[116]Ibid., 18.
[117]Ibid.
[118]Ibid., 32-34.
[119]Ibid., 36.

understanding however; the uniqueness of each individual locality highlights the need for local commanders to have the requisite authority for IO message development. Within that commander's authority resides the responsibility to ensure the message is nested within the higher command's themes in order to prevent message conflict. However, failure to grant that authority may likely result in IO messages which will have no chance of resonation with the local populace.

The method of message delivery and the consistency of action by the COIN force are also of critical importance to the credibility and resonation of the IO campaign.[120] The use of local leaders and even of non-governmental organizations to assist in message delivery may significantly impact the willingness of the population to receive and propagate the message. Even the force's engagement of the local or regional media may have a positive effect on the population's perception of credibility.[121]

Along with these efforts to connect to the population through local legitimacy, the COIN forces must also be aware of the consistency of their own actions and messages. Soldiers and Marines' actions, reactions, attitude and posture on the ground will create perceptions in the minds of the population which will either reinforce or undermine the credibility and coherence of the force's IO.[122] Further, as units conduct relief in place and rotate out or unit boundaries change, population expectations for how the new unit conducts operations and the nature of the messages it promotes will certainly affect the credibility of the new force and its IO campaign.[123]

The many framing considerations for the information environment provided by the workshop report highlight the broad scope of issues which must be considered or addressed by the COIN force commander and staff. Again, despite the Israeli-Palestinian context in which

---

[120]Ibid., 38.
[121]Ibid.
[122]Ibid., 41.
[123]Ibid., 42.

these considerations were developed, they remain relevant and timeless to COIN forces executing

operations today, and are a critical component of gaining a comprehensive understanding of the

information environment.

CHAPTER SIX
RECOMMENDATIONS AND CONCLUSION

This monograph thesis set out to explore the role of IO within contemporary operations with the goal of identifying several reasons why commanders and staffs have been challenged to fully integrate IO in the ongoing COIN operations. The research for the paper highlighted several deficiencies for IO within doctrine, organizational structure, training, material and personnel. These deficiencies will be briefly described individually with recommendations provided to address each one.

Recommendations

The first recommendation derived from the research is the need for US Army IO doctrine to fully nest within the framework provided by the joint publication. This appears to be an inherent requirement; however the review of service doctrine within this monograph has demonstrated that this requirement is not always adhered to by the various service doctrine writers. The Army has yet to publish an updated version of its IO manual, FM 3-13 to coincide with the new JP 3-13. However, as the review of FM 3-24 indicated, the IO focus within the Army appears to have shifted away from the EW spectrum and more towards the elements that reside in the cognitive domain of the information environment. The Army's potential imbalance of IO focus could create friction as US operations continue to feature more joint and interagency integration at lower echelons of command. Thus it is imperative that the Army IO doctrine complies with the joint framework.

Another doctrinal application which requires greater attention is the adequate integration of IO across the LLOs within COIN. Although FM 3-24 highlighted many of the tasks necessary to integrate IO into all LLOs within COIN, the manual did not address how this is necessarily accomplished within the day to day operations of the headquarters. A critical requirement for full

integration is the elevation of importance of all the traditional non-lethal contributors to the effects working group (EWG). The officers and non-commissioned officers (NCOs) of these staff sections have traditionally been relegated to the seats in the back of the tactical operations centers (TOCs). The increase of relative importance of IO requires that these individuals can no longer operate in the background. In order to ensure IO is properly integrated within all LLOs, these critical players must be afforded a voice and a seat at the head table of the headquarters' daily targeting meetings.[124] Without the appropriate value attributed to these important staff contributors, IO will likely not reach full integration across all LLOs.

A deficiency which has implications on the commander and staff's ability to fully integrate IO within COIN operations is the insufficient IO education and training afforded to the Soldiers, NCOs and officers of the force. As noted in chapter three, there is a distinct lack of dedicated attention to IO education in the Army's junior and mid-career level service schools. While the IO Roadmap has addressed the education deficiency at the senior service college level[125], more attention must be directed towards the officers who will fill the staff positions of the operational and tactical level commands. This additional requirement implies that Training and Doctrine Command (TRADOC) will be afforded the requisite number of IO school trained officers to provide this necessary education to junior and mid-career officers. Because the IO career field is and will continue to be understrength through 2013, an alternative solution is to send selected officers of all branches to the joint or service specific IO courses en-route to their instructor or staff assignments. This alternative solution would not only alleviate the strain on the IO career field officers, but would also quickly resolve much of the existing misunderstanding of IO within the force.

---

[124]MG David Fastabend, "EBO and the Classical Elements of Operational Design," US Army Futures Center PowerPoint Presentation dated 31 January 2006, notes of slide 9.
[125]DoD, IO Roadmap, 12.

The next deficiency to address is the Army's ability to conduct adequate assessment of IO's effectiveness. This deficiency has implications on the systems and databases available to assemble and analyze the IO assessments. As stated in chapter five, the Army's systems for assessment and analysis of MOE within the information environment exist in both the MI and the IO communities. While each may depend heavily on the other in the analysis and assessment of the COIN environment, the two systems are incompatible and require additional coordination to complete a comprehensive analysis. Further, the additional layer of coordination between the two communities adversely affects the timeliness of the analysis and the force's ability to adapt the IO campaign to changing conditions. To resolve this deficiency, the IO community requires a networked database system which is both similar to and compatible with the intelligence community's ASAS network.

The final recommendation resides in each COIN force's need to assume a proactive posture during the conduct of its IO campaign. This proactive posture is predicated on the commander's acknowledgement of IO's relative importance to the kinetic operations in the COIN environment. As discussed in the workshop report in chapter five, the COIN force must consider and develop the shaping messages and IO effects for both before and after the execution of kinetic operations to prevent insurgent attempts to undermine the legitimacy of the unit's efforts.[126] Further, COIN forces and their leaders must remain fully engaged with the media, both foreign and domestic. By engaging the local, foreign and international media quickly and as accurately as possible following an action or incident, the COIN force will preclude the insurgent force from gaining the informational advantage by propagating harmful rumors.[127] This posture is critical to the legitimacy and the overall success of the COIN effort.

---

[126]Collings and Rohozinski, 17.
[127]COL Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review*, May-June 2006, 18.

Conclusion

As the US and its coalition partners continue to pursue COIN operations in Iraq and Afghanistan, it is clear that IO has taken on a new level of importance to the success of the campaigns. Due to the inherently political nature of COIN and the vast fungibility of information in the global information environment, IO can no longer remain as merely a supported or shaping operation. Commanders must recognize this relationship and work to balance their efforts and understanding within the physical and informational battlespace.

Although new Joint IO and Army COIN doctrine have provided a solid foundation for understanding of the necessities of this current conflict, several issues remain. For the existing deficiencies within doctrine, organization, material, training and personnel, US forces must continue to maintain its ingenuity in developing creative solutions to these issues. Development of viable new tactics, techniques and procedures will continue to drive the refinement of doctrine as well as organizational and material needs so that commanders will have the resources they need to properly integrate IO. Perhaps the ideas and recommendations presented within this monograph will help commanders overcome these deficiencies, allowing their units to become more viable forces within the information environment.

BIBLIOGRAPHY

Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power.*
Washington, D.C.: Brassey's, Inc, 2004.

Baker, Ralph O. "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on
Information Operations." *Military Review,* May-June 2006, 13-32.

Barno, David W. "Challenges in Fighting a Global Insurgency." *Parameters,* Summer 2006, 15-
29.

Belknap, Margaret. "The CNN Effect: Strategic Enabler or Operational Risk?" *Parameters,*
Autumn 2002, 100-114.

Center for Army Lessons Learned Handbook. *Tactical Commander's Handbook, Information
Operations (OIF).* Fort Leavenworth, KS: US Army Combined Arms Center, 2005.

Celeski, Joseph D. "COIN Strategic Aspects of Counterinsurgency." *Military Review,* March-
April 2006, 35-41.

Chandler, David G. *The Campaigns of Napoleon.* New York: MacMillan Publishing, 1966.

Cohen, Ariel. "Promoting Freedom and Democracy: Fighting the War of Ideas against Islamic
Terrorism." *Comparative Strategy,* July, August, September 2003.

Collings, Deirdre and Rafal Rohozinski. "Shifting Fire: Information Effects in
Counterinsurgency and Stability Operations." Center for Strategic Leadership Workshop
Report, Carlisle, PA., November 2006.

Cronin, Audrey Kurth. "Cyber-Mobilization: The New Levee en Masse." *Parameters,* Summer
2006, 77-87.

Cox, Joseph L. "Information Operations in Operations Enduring Freedom and Iraqi Freedom –
What Went Wrong?" Monograph, US Army Command and General Staff College,
School of Advanced Military Studies, AY 05-06, Fort Leavenworth, KS.

Davis, Jacquelyn, K. "Radical Islamist Ideologies and the Long War: Implications for U.S.
Strategic Planning and U.S. Central Command's Operations." *Institute for Foreign
Policy Analysis Inc. and Defense Threat Reduction Agency White Paper,* Washington,
DC, January 2007.

Darley, William Colonel. "Clausewitz's Theory of War and Information Operations." *Joint
Force Quarterly,* iss. 40, 1st Quarter 2006, 73-79.

_____. "War Policy, Public Support and the Media." *Parameters,* Summer 2005, 121-134.

De Atkine, Norvell B. "Why Arabs Lose Wars." *American Diplomacy: Middle East Quarterly,*
vol. 6, no. 2., December 1999.

Eassa, Charles N. "US Armed Forces Information Operations – Is the Doctrine Adequate?"
Monograph, US Army Command and General Staff College, School of Advanced
Military Studies, AY 99-00, Fort Leavenworth, KS.

Fastabend, David, Major General. "EBO and the Classical Elements of Operational Design." US
Army Futures Center PowerPoint Presentation dated 31 January 2006, 22 slides.

Ford, Christopher. "Speak No Evil: Targeting a Population's Neutrality to Defeat an Insurgency." *Parameters*, Summer 2005, 51-66.

Galula, David. *Counterinsurgency Warfare Theory and Practice.* St Petersburg FL: Hailer Publishing, 2005.

Griffith, Samuel B, (Translation). *The Art of War, Sun Tzu.* New York: Oxford University Press, 1963.

Grohoski, David C., Steven M. Seybert, and Marc J. Romanych, Marc J. "Measures of Effectiveness in the Information Environment." *Military Intelligence Professional Bulletin,* July-September 2003, 12-16.

Grubbs, Lee, Major and Major Michael Forsyth. "Is There a Deep Fight in a Counterinsurgency?" *Military Review*, July-August 2005, 28-31.

Hall, Wayne Michael. *Stray Voltage: War in the Information Age.* Annapolis MD: Naval Institute Press, 2003.

Handel, Michael I. *Clausewitz and Modern Strategy.* London: London Cass, 1986.

Hoffman, Bruce. "Insurgency and Counterinsurgency in Iraq." Arlington, VA: RAND, National Security Research Division, Occasional Paper -127-IPC/CMEPP, June 2004.

Jones, Jeffrey. "Strategic Communication: A Mandate for the United States." *Joint Force Quarterly*, iss. 39, 3rd Quarter, 2005.

Kagan, Frederick W. "Measuring Success." *Armed Forces Journal International*, January 2006, vol. 143 iss. 6, 20-24.

Keeton, Pamela and Mark McCann. "Information Operations, STRATCOM, and Public Affairs." *Military Review*; November-December 2005, vol. 85 iss. 6, 83-86.

Kelly, Stephanie R. "Rumors in Iraq: A Guide to Winning Hearts and Minds." Thesis, Naval Post Graduate School, Naval War College, September 2004.

Lamb, Christopher J. "Information Operations as a Core Competency." *Joint Force Quarterly*, December 2004, 88-96.

Mattis, James Lieutenant General and Lieutenant Colonel (Retired) Frank Hoffman. "Future Warfare: The Rise of Hybrid Wars." *Proceedings Magazine*, November 2005, 18-19.

McDaniel, Erin A., Perez, Julio A. How to Visualize and Shape the Information Environment. Ft. Sill, OK: Field Artillery Magazine, November-December 2006. p26-33.

Meigs, Montgomery General (Retired). "Unorthodox Thoughts about Asymmetric Warfare." *Parameters,* Summer 2003, 4-18.

Murray, William S. "A Will to Measure: Measures of Effectiveness in Military Decision-making." *Parameters*, Autumn 2001, 134-147.

Nagl, John A. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam.* Chicago, IL: The University of Chicago Press, 2005.

_____. "New Rules for New Enemies." *Armed Forces Journal*, October 2006. 25-31, 52-56.

O'Neill, Bard E. *Insurgency & Terrorism: Inside Modern Revolutionary Warfare.* Dulles VA: Brassey's Inc., 1990.

Patai, Raphael. *The Arab Mind.* New York: Hatherleigh Press, 2002.

Payne, Kenneth. "The Media as an Instrument of War." *Parameters,* Spring 2005, 81-93.

Peters, Ralph. "Progress and Peril: New Counterinsurgency Manual Cheats on the History Exam." *Armed Forces Journal,* February 2007, 34-37.

Record, Jeffrey. "Why the Strong Lose." *Parameters,* Winter 2005-2006, 16-31.

Rhodes, J. E. "A Concept for Information Operations." *Marine Corps Gazette,* August 1998, A1-A10.

Rosenau, William. *Winning the War of Ideas.* Washington, DC: RAND National Strategic Research Division, Date Unknown.

Schleifer, Ron. "Reconstructing Iraq: Winning the Propaganda War in Iraq." *Middle East Quarterly,* Summer 2005, vol. 12 iss. 3, 1-10.

Tomes, Robert R. "Relearning Counterinsurgency Warfare." *Parameters,* Spring 2004, 16-28.

TRADOC Pamphlet 525-69. *Military Operations: Concept for Information Operations.* 1 August 1995.

Trinquier, Roger. *Modern Warfare A French View of Counterinsurgency.* London and Dunmow. Pall Mall Press, 1961 (Daniel Lee Translator).

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations.* 6th ed. Chicago: University of Chicago Press, 1996.

Von Clausewitz, Carl. *On War.* New Jersey: Princeton University Press, 1976 (Howard Michael and Peter Paret Editors/Translators).

U.S. Department of Defense. *Information Operations Roadmap.* 30 October 2003

U.S. Department of Defense Directive (DODD) 3222.4. *Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures.* 31 July 1992.

U.S. Army FM 3-0. *Operations.* 14 June 2001.

U.S. Army FM 3-13. *Information Operations: Doctrine, Tactics, Techniques and Procedures.* 28 November 2003.

U.S. Army FM 6-0. *Mission Command: Command and Control of Army Forces.* 11 August 2003.

U.S. Army FMI 3-07.22. *Counterinsurgency Operations.* 1 October 2004.

U.S. Army FM 3-24. *Counterinsurgency Operations.* 15 December 2006.

U.S. Army FM 100-6. *Information Operations.* 27 August 1996

U.S. Department of Defense Joint Pub 3-0. *Doctrine for Joint Operations.* 17 September 2006.

U.S. Department of Defense Joint Pub 3-13. *Information Operations.* 13 February 2006.

U.S. Department of Defense Joint Pub 5-0. *Doctrine for Planning Joint Operations.* 3rd draft 10 August 2005.

General Reference

http://www.au.af.mil/au/aul/bibs/asw.htm

http://www.carlisle.army.mil/usacsl/Studies.asp

http://www.iwar.org.uk/index.htm

http://www.jfcom.mil/about/fact_ona.htm